

CLAIMS

1. A method for establishing an affiliation within a single sign-on system, comprising the steps of:

5 defining a group of service providers that act as a single entity on a network for purposes of any of authentication, federation, and authorization;

 defining an owner of said affiliation that is responsible for maintaining a list that shows which service providers are members of said affiliation, as well as any control structure or meta-data associated with said affiliation; and

10 providing a unique identifier for each affiliation within said single sign-on system in which said affiliation is defined.

2. The method of Claim 1, wherein said network comprises:

15 a web services-based service infrastructure in which users manage sharing of their personal information across identity providers and service providers.

3. The method of Claim 2, wherein said web services implement a lightweight protocol for exchange of information in a decentralized, distributed environment.

20 4. The method of Claim 3, wherein said protocol comprises:

 an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses.

25

5. An apparatus for establishing an affiliation within a single sign-on system, comprising:

a plurality of principals that can acquire a federated identity and be authenticated and vouched for by an identity provider;

5 an identity provider for authenticating and vouching for principals;

a plurality of service providers that act as a single entity with regard to authentication, federation and authorization to establish a single sign-on system within which such affiliation cooperates; and

10 at least one service associated with each service provider which comprises a grouping of common functionality comprising at least one method that callers can use to manipulate information managed by said service with regard to a particular principal.

6. The apparatus of Claim 5, further comprising:

15 a web service provider for hosting personal web services which invoke web service methods at said web service provider.

7. The apparatus of Claim 6, further comprising:

20 a web service consumer for accessing a user's personal web services by communicating with said web service provider.

8. The apparatus of Claim 7, further comprising:

a discovery service for enabling said web service consumer to discover service information regarding a user's personal web services.

25

9. A method for establishing an affiliation within a single sign-on system, comprising the steps of:

defining a group of service providers that act as a single entity on a network for purposes of any of authentication, federation, and authorization;

5 providing a plurality of principals that can acquire a federated identity and be authenticated and vouched for by an identity provider; and

providing an identity provider for authenticating and vouching for principals.

10. The method of Claim 9, further comprising the steps of:

10 a principal logging into said identity provider;

said principal visiting a first service provider and federating to said group; and

said principal then visiting any other service provider within said group.

11. The method of Claim 9, further comprising the step of:

15 defining an owner of said affiliation that is responsible for maintaining a list that shows which service providers are members of said affiliation, as well as any control structure or meta-data associated with said affiliation.

12. The method of Claim 9, further comprising the step of:

20 providing a unique identifier for each affiliation within said single sign-on system in which said affiliation is defined.

13. The method of Claim 9, further comprising the step of:

25 providing a discovery service for enabling a web service consumer to discover service information regarding a user's personal web services.

14. The method of claim 13, further comprising the step of:

providing a web service consumer associated with a service provider for requesting a service descriptor and assertion for service from said discovery service and for presenting an assertion from said other service provider with affiliate
5 information.

15. The method of Claim 14, further comprising the step of:

said discovery service checking said other service provider affiliation and generating a service assertion based upon said other service provider affiliation.

16. The method of Claim 15, further comprising the step of:

said web service consumer invoking a service with said service assertion via a web service provider.

17. The method of Claim 9, wherein said group has an identifier that is unique within a single sign-on system in which said group is defined.

18. The method of Claim 9, wherein service providers within a single sign-on system may be members of multiple groups, but can only act with a single affiliation for any
20 given transaction.

19. The method of Claim 9, wherein a user federating with a group automatically federates with all members of said group.

20. The method of Claim 9, wherein a user authorizing access to a service by said federation authorizes access to any member of said group.

21. The method of Claim 9, further comprising the step of:

providing a unique identifier for any service provider/group affiliation. wherein
if a same service provider using a same service provider identity requests an identity
of a user through different group affiliations, said service provider receives different,
5 unique identifiers for each group affiliation.

22. The method of Claim 9, further comprising the step of:

providing a same identifier to all members of said group when they are acting
as a part of said group affiliation.

10

23. The method of Claim 9, further comprising the step of:

providing an affiliation name identifier for allowing sites to handle an automatic
federation that take place with all members of said group.

15

20

25